CARD/READER INTEROPERABILITY REQUIREMENT GUIDELINES

General Services Administration

July 10, 2006

Document Version: 5.0

TABLE OF CONTENTS

1. INTRODUCTION

The purpose of this document is to define and validate a suite of performance, interoperability and security requirements for PIV Card and Reader interface associated with a Personal Identity Verification (PIV) System consistent with Federal Information Processing Standards (FIPS) Publication 201 and its associated documents. This document is not intended to re-state or contradict requirements specifically identified in FIPS 201 or its associated documents. It is intended to augment existing standards to enable agencies to achieve the interoperability goal of Homeland Presidential Security Directive 12 (HSPD).

Section two provides requirements that facilitate interoperability between any card and any reader (physical or logical operating environment). Performance-based requirements that enable rapid electronic authentication are listed in section three and requirements pertaining to security in a moderate risk environment are listed in section four.

2. CARD / READER INTEROPERABILITY REQUIREMENTS

2.1. PIV Card

2.1.1. Contact Interface

2.1.1.1. Programming Voltage

Requirement – PIV Cards shall not require a Programming Voltage to operate correctly.

Rationale – This mirrors a requirement from paragraph 3.1.2 of the Personal Computer / Smart Card (PC/SC) Specification. Over 500 readers from more than 50 manufacturers voluntarily conform with the PC/SC Specification. Paragraph 4.5.1 of FIPS 201 requires that the reader-to-host system interface for a reader in the general desktop computing environment conform with the PC/SC specification but it does not require that the card-to-reader interface conform.

2.1.1.2. Operating Class

Requirement - PIV cards shall support the Class A operating class as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.

Rationale – ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002 provide for three operating classes, Class A (5v), Class B (3v) and Class C (1.8v). Compliant cards and readers may support one or more consecutive classes. Requiring support for the class A operating class will guarantee interoperability. Not allowing Class B and Class C cards or readers will ensure there are no incompatible card/reader combinations.

2.1.1.3. Transmission Protocol

Requirement – At a minimum, PIV Cards shall support either the T=0 or T=1 transmission protocol as defined in ISO/IEC 7816-3:1997. The card may support both protocols.

Rationale – ISO/IEC 7816-3:1997 provides for 15 transmission protocols, two of which are defined in the standard. The remaining protocols are reserved for future use or are not standardized by ISO/IEC Joint Technical Committee (JTC) 1 Steering Committee (SC) 17. Provided readers support both protocols, interoperability can be guaranteed by requiring PIV cards support at least one of the two protocols.

2.1.1.4. Reserved for Future Use (RFU) Bits

Requirement – PIV Cards shall not require the use of any RFU bits in the Global or Specific Interface Bytes to operate correctly.

Rationale – ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002 reserve several bits in the Global and Specific Interface Bytes for future use. Although these bits have been reserved, their use is not prohibited. Vendors may use them to define unique features that are not part of the standard. These unique features may not be supported by other vendors and may negatively impact card / card reader interoperability.

2.1.2. Contactless Interface

Requirement - PIV Card Contactless interfaces shall comply with FIPS 201 and supporting documentation.

Rationale – No additional requirements other than those defined in FIPS 201 and supporting documentation, are required to enable a reader to read data from a PIV Card.

2.2. PIV Reader

2.2.1. Contactless Interface (logical or physical)

2.2.1.1. Type A and B Communication Signal Interfaces

Requirement - The contactless interface of the reader shall support both the Type A and Type B communication signal interfaces as defined in ISO/IEC 14443-2:2001.

Rationale – If the reader does not support both communication signal interfaces defined in ISO/IEC 14443-2:2001, Type B cards could not be read by Type A readers. The same holds true for Type A cards with type B readers.

2.2.1.2. Type A and B Initialization and Anti-Collision

Requirement - The contactless interface of the reader shall support both Type A and Type B initialization and anti-collision methods as defined in ISO/IEC 14443-3:2001.

Rationale – If the reader does not support both methods defined in ISO/IEC 14443-3:2001, Type B cards could not be read by Type A readers. The same holds true for Type A cards with type B readers.

2.2.1.3. Type A and B Transmission Protocols

Requirement - The contactless interface of the reader shall support both Type A and Type B transmission protocols as defined in ISO/IEC 14443-4:2001.

Rationale – If the reader does not support both transmission protocols defined in ISO/IEC 14443-4:2001, Type B cards could not be read by Type A readers. The same holds true for Type A cards with type B readers.

2.2.2. Contact Interface (logical or physical)

2.2.2.1. Operating Class

Requirement - PIV readers shall support the Class A operating class as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.

Rationale – ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002 provide for three operating classes, Class A (5v), Class B (3v) and Class C (1.8v). Compliant cards and readers may support one or more consecutive classes. Requiring support for the class A operating class will guarantee interoperability. Not allowing Class B and Class C cards or readers will ensure there are no incompatible card/reader combinations.

2.2.2.2. Transmission Protocol

Requirement - The contact interface of the reader shall support both the T=0 and T=1 transmission protocols as defined in ISO/IEC 7816-3:1997.

Rationale – ISO/IEC 7816-3:1997 provides for 15 transmission protocols, two of which are defined in the standard. The remaining protocols are reserved for future use or are not standardized by ISO/IEC JTC 1 SC 17. Under PC/SC specifications, cards must support T=0 or T=1 and they may support both. Provided cards conform with the PC/SC specification, requiring readers that support both protocols will guarantee interoperability. The physical reader to physical access control panel interface is not defined so in order to support interoperability the transmission protocol for physical readers must be definitive.

2.2.2.3. Modes of Operation

Requirement - PIV Readers shall support implicit protocol and parameter selections (PPS) as defined in ISO/IEC 7816-3:1997.

Rationale – This allows the card and reader to operate using default values when parameters are not provided in specific interface bytes. Section 6.6.3 of ISO/IEC 7816-3 allows the option of not supporting PPS.

3. ELECTRONIC AUTHENTICATION PERFORMANCE REQUIREMENTS

3.1. PIV Card

3.1.1. Contactless Interface

3.1.1.1. Retrieval Time

Requirement - Retrieval time (does not include activation/deactivation of PIV card electrical circuits by the “golden” reader) for 266 bytes of data through the contactless interface of the card shall not exceed 500 milliseconds when coupled with a “golden reader” that is operating at 106kbits/sec.

Rationale - The retrieval time (does not include activation/deactivation of PIV card electrical circuits by the “golden” reader) for the contactless interface in section 3.1 is based on the length of the CCC, which is the only mandatory buffer in the PIV data model that is accessible from that interface. It has a maximum length of 266 bytes. Assuming a 50% overhead, a maximum of 512 bytes of information will be sent through the contactless interface Contact Interface

3.2. PIV Reader

3.2.1. General

3.2.1.1. Buffer Size

Requirement - The reader buffer size shall be no less than 256 bytes.

3.2.2. Contactless Interface

3.2.2.1. Bit Rate

Requirement - The contactless interface of the reader shall support bit rates of *fc*/128 (~106 kbits/s), *fc*/64 (~212 kbits/s), *fc*/32 (~424 kbits/s) and *fc*/16 (~847 kbits/s) as defined in ISO/IEC 14443-3:2001/Amd.1:2005

Rationale – ISO/IEC 14443-3:2001/Amd.1:2005 defines one mandatory and three optional bit rates for communication. If the reader fully supports all four rates, the highest speed available on the card can be used to increase authentication and authorization times.

3.2.3. Contact Interface

3.2.3.1. Protocol and Parameter Selection

Requirement – PIV readers shall support the Protocol and Parameters Selection (PPS) protocol as defined in ISO/IEC 7816-3:1997.

Rationale – The PPS protocol allows a reader to propose a different protocol or values for the clock rate conversion and baud rate adjustment factors that may be supported by the card. A successful PPS exchange will result in improved data transfer speeds.

4. SECURITY RELATED REQUIREMENTS

4.1. PIV Card

4.1.1. Contactless Interface

4.1.1.1. Skimming

Requirement - Buffers shall not be readable through the contactless interface when the card is stored in an electromagnetically opaque sleeve at any distance.

Rationale –The purpose of this requirement is to prevent the disclosure of unprotected data on the contactless side of the card.

4.2. PIV Reader

4.2.1. Contactless Interface

4.2.1.1. Eavesdropping

Requirement - Buffers shall not be readable through the contactless interface more than 10 cm from the reader.

Rationale – The contactless interface specified in ISO 14443 parts 1 through 4 generate limited field strengths that limit read distance by design. There are many factors that determine the actual read distance making it difficult to establish an actual number. Ten centimeters has been the most widely accepted maximum distance but it is not referenced in any authoritative specification.

5. REFERENCES

The following references were used in the preparation of this document:

IEEE 802.3-2005, Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks--Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications

ISO/IEC 7816-3:1997 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols

ISO/IEC 7816-3:1997/Amd. 1:2002 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols AMENDMENT 1: Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1.8 V

ISO/IEC 14443-2:2001 Identification cards - Contactless integrated circuit(s) cards – Proximity cards - Part 2: Radio frequency power and signal interface

ISO/IEC 14443-3:2001/Amd.1:2005 Identification cards – Contactless integrated circuit(s) cards – Proximity cards Part 2: Radio frequency power and signal interface AMENDMENT 1: Bit rates of *fc* /64, *fc* /32 and *fc* /16

Interoperability Specification for ICCs and Personal Computer Systems Part 2. Interface Requirements for Compatible IC Cards and Readers, Revision 2.01.02, September 2005

SIA Access Control Standard Protocol for the 26-BIT Wiegand™ Reader Interface, October 17, 1996

TIA-232 Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange, Revision F, October 11, 2002

TIA-485 Electrical Characteristics of Generators and Receivers For Use in Balanced Digital Multipoint Systems, Revision A, March 28, 2003

6. DEFINITIONS

Global Interface Byte — A byte in the Answer to Reset (ATR) sequence that refers to parameters of the integrated circuit or circuits within a card

Retrieval Time — The time to retrieve a specified amount of data.

Specific Interface Byte	A byte in the ATR sequence that refers to the parameters of a transmission protocol offered by a card.

7. ABBREVIATIONS AND ACRONYMS

ATR	Answer to Reset
CHUID	Card Holder Unique Identifier
FASC-N	Federal Agency Smart Card Number
FIPS	Federal Information Processing Standards
HSPD	Homeland Security Presidential Directive
ICC	Integrated Circuit Chip
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical & Electronics Engineers
ISO	International Organization for Standardization
JTC	Joint Technical Committee
KB	Kilobyte
NIST	National Institute of Standards and Technology
PC/SC	Personal Computer / Smart Card
PIV	Personal Identification Verification
PPS	Protocol and Parameters Selection
RFU	Reserved for Future Use
SIA	Security Industry Association
SC	Steering Committee
TIA	Telecommunications Industry Association
VCC	Voltage at the Common Collector